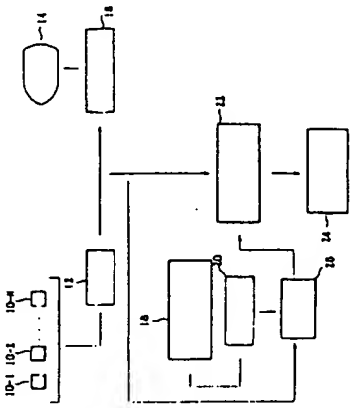
(54) VISUAL IC CARD
(11) 4-255089 (A) (43) 10.9.1992 (19) JP
(21) Appl. No. 3-36674 (22) 6.2.1991
(71) FUJITSU LTD (72) HIROSHI TANAKA
(51) Int. Cl⁵. G06K19/10,B42D15/10,G06K19/07

PURPOSE: To provide an extremely effective visual IC card having many functions and excellent security with respect to an ID card to be used for a cash card, a credit card, a medical card, etc., especially provided with an input key and a display device.

CONSTITUTION: A data input means 12 inputs data corresponding to the operation of keys 10-1 to 10-N and an input data display means 16 displays the inputted data on a display device 14. Plural applications are previously written in an application storing means 18 and an identification(ID) data storing means 20 previously stores application ID data. A data collating means 22 collates the inputted data with the application ID data and a person-confirming means 24 confirms a card user as the owner when a positive collated result is obtained.

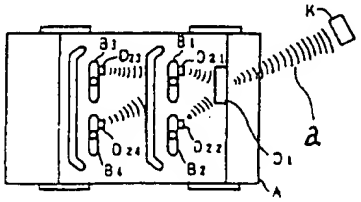


26: ID data reading means

(54) IDENTIFICATION SYSTEM FOR VEHICLE IN/OUT MANAGEMENT
(11) 4-255090 (A) (43) 10.9.1992 (19) JP
(21) Appl. No. 3-9585 (22) 30.1.1991
(71) MEIDENSHA CORP (72) KAZUYUKI KUMAKI
(51) Int. Cl⁵. G07C9/00,B42D15/10,G06F15/21,G06K17/00,G08G1/017

PURPOSE: To automatically execute vehicle identification(ID) and the personal ID of a person getting on a vehicle and to simplify management by making a vehicle ID device loaded on a vehicle to inquire a personal ID card carried by a person getting on the vehicle at the time of passing a gate and transmit a personal ID code together with a vehicle ID code to a vehicle detector.

CONSTITUTION: When a vehicle A passes a gate, the vehicle detector K sends an access signal to a vehicle ID device D_t. The device D_t transmits an inquiry signal from a transmission part to the inside of the vehicle at the period of about one minute. Persons B_1 to B_4 getting on the vehicle respectively carry respective personal ID cards D_{21} or the like. After receiving the inquiry signal, respective cards D_{21} or the like transmit personal ID codes. Each personal ID card is provided with an inherent queue time based on a registered number to prevent the generation of signal collision. The device D_t transmits the vehicle ID code and the personal ID codes to the detector K. The detector K manages the IN/OUT of the vehicle and the persons getting on the vehicle in accordance with these codes.

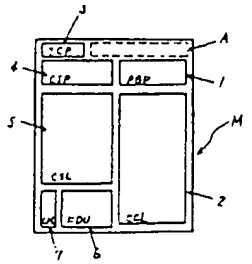


a: signal wave

(54) CASH DISPENSER
(11) 4-255091 (A) (43) 10.9.1992 (19) JP
(21) Appl. No. 3-36901 (22) 6.2.1991
(71) NEC CORP (72) YOSHIMI KITAGAWA
(51) Int. Cl⁵. G07D1/00,G07D9/00

PURPOSE: To improve the operation convenience of a cash dispenser by providing the cash dispenser body with a consumption medium stock rack for storing consumption medium so as to always store the consumption medium.

CONSTITUTION: The cash dispenser body M is provided with a bankbook printer unit 1, a paper money processing unit 2, a card processing unit 4, or the like. The consumption medium stock rack A is arranged on a space position in the upper area of the dispenser body M. The stock rack A is formed by reinforced glass or reinforced plastic so that the inside can be observed and the number of remaining medium can be checked at a glance from the external. The stock rack A is laterally arranged and provided with a bankbook storing rack, a certificate storing rack, a receipt form storing rack, a journal form storing rack, a depositing/paying form storing rack, and a transfer card storing rack. Respective racks are provided with locking keys so as to store important medium.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平4－255089

(43)公開日　平成４年(1992)９月10日

Published

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｋ　19/10				
Ｂ４２Ｄ　15/10	５２１	9111－2Ｃ		
Ｇ０６Ｋ　19/07				
		8623－5Ｌ	Ｇ０６Ｋ　19/00	Ｒ
		8623－5Ｌ		Ｊ

審査請求　未請求　請求項の数３(全　６　頁)

(21)出願番号　特願平3－36674

(22)出願日　平成３年(1991)２月６日

Application Date　Feb. 6, 1991

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中1015番地

(72)発明者　田中　弘
神奈川県川崎市中原区上小田中1015　富士通株式会社内

(74)代理人　弁理士　伊藤　儀一郎

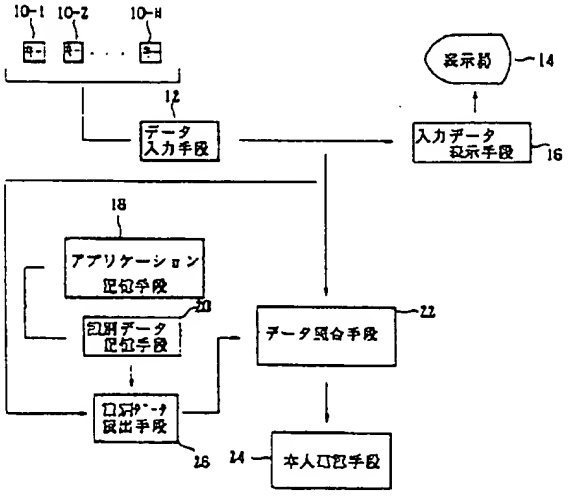
(54)【発明の名称】　ビジュアルＩＣカード

(57)【要約】

【目的】　本発明は、キャッシュカード，クレジットカード，医療カードなどに利用されるＩＣカードにかかり、特に、入力キーと表示器が設けられたＩＣカードに関し、多機能でセキュリティに優れた極めて有用なビジュアルＩＣカードの提供を目的とする。

【構成】　キー１０－１，１０－２・・・１０－Ｎの操作に応じたデータをデータ入力手段１２が入力し、入力データ表示手段１６は入力されたデータを表示器１４に表示させる。アプリケーション記憶手段１８には複数のアプリケーションが予め書き込まれ、識別データ記憶手段２０はアプリケーション識別用のデータを予め記憶する。データ照合手段２２は入力されたデータをアプリケーションの識別データと照合し、本人確認手段２４は肯定的な照合結果が得られたときにカード利用者の本人確認を行なう。

発明の原理説明図



1

【特許請求の範囲】

【請求項1】　キー（10－1，10－2・・・10－N）の操作に応じたデータを入力するデータ入力手段（12）と、入力されたデータを表示器（14）に表示させる入力データ表示手段（16）と、複数のアプリケーションが予め書き込まれたアプリケーション記憶手段（18）と、アプリケーション識別用のデータを予め記憶する識別データ記憶手段（20）と、入力されたデータをアプリケーションの識別データと照合するデータ照合手段（22）と、肯定的な照合結果が得られたときにカード利用者の本人確認を行なう本人確認手段（24）と、を有する、ことを特徴としたビジュアルＩＣカード。

【請求項2】　キー（10－1，10－2・・・10－N）の操作に応じアプリケーション特定データとアプリケーション固有データを入力するデータ入力手段（12）と、入力されたデータを表示器（14）に表示させる入力データ表示手段（16）と、複数のアプリケーションが予め書き込まれたアプリケーション記憶手段（18）と、アプリケーション識別用のデータを予め記憶する識別データ記憶手段（20）と、入力されたアプリケーション特定データと対応したアプリケーション識別用のデータを読み出す識別データ読出手段（26）と、入力されたアプリケーション固有データを読み出されたアプリケーション識別用のデータと照合するデータ照合手段（22）と、肯定的な照合結果が得られたときにカード利用者の本人確認を行なう本人確認手段（24）と、を有する、ことを特徴としたビジュアルＩＣカード。

【請求項3】　キー（10－1，10－2・・・10－N）の操作に応じアプリケーション特定データとアプリケーション固有データを入力するデータ入力手段（12）と、入力されたデータを表示器（14）に表示させる入力データ表示手段（16）と、複数のアプリケーション記憶手段（18）と、アプリケーション識別用のデータを予め記憶する識別データ記憶手段（20）と、入力されたアプリケーション特定データと対応したアプリケーション識別用のデータを読み出す識別データ読出手段（26）と、入力されたアプリケーション固有データを読み出されたアプリケーションの識別データと照合するデータ照合手段（22）と、肯定的な照合結果が得られたときに該当のアプリケーションについてのみカード利用者の本人確認を行なう本人確認手段（24）と、を有する、ことを特徴としたビジュアルＩＣカード。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、キャッシュカード，クレジットカード，医療カードなどとして利用されるＩＣカードにかかり、特に、入力キーと表示器が設けられたＩＣカードに関する。

2

【0002】この種のＩＣカードには入力キーと表示器が設けられており、したがって、それらを用いてカード利用者の本人確認をカード単体で行なうことが可能となる。

【0003】

【従来の技術】図11にはＩＣカードシステムが示されており、キーボード80が処理装置82（パーソナルコンピュータなど）に設けられている。

【0004】この処理装置82にはカードリーダ・ライタ84が接続されており、ＩＣカード86はカードリーダ・ライタ84にセットされる。

【0005】そして、キーボード80の操作で処理装置82にＰＩＮデータが入力されると、この入力データがＩＣカード86へ送信される。

【0006】その結果、カード利用者の本人確認が行なわれると、ＩＣカード86を利用した取引が行なわれる。

【0007】ところがこのシステムにおいては、本人確認用のＰＩＮデータが処理装置82へ入力されるので、ＰＩＮデータの漏洩を確実に防止することが困難となる。

【0008】そこで、図2のように複数のキー10と表示器14とを備え、これらキー10，表示器14によってカード利用者の本人確認をカード単体で行なえるビジュアルＩＣカード28が利用される。

【0009】従来においては、ビジュアルＩＣカード28に単一のアプリケーションが用意されており、したがって、その用途はキャッシュカード，クレジットカード，医療カードなどのいずれかに限られていた。

【0010】

【発明が解決しようとする課題】ＭＳカード（磁気カード）にはキャッシュカード，クレジットカードの機能が既に付与されているので、これより能力がはるかに高いビジュアルＩＣカード（28）にはより豊富な機能が要望される。

【0011】本発明は上記従来の事情に鑑みてなされたものであり、その目的は、ＰＩＮデータの漏洩を確実に防止できる多機能なビジュアルＩＣカードを提供することにある。

【0012】

【課題を解決するための手段】上記目的を達成するために、本発明にかかるビジュアルＩＣカード（28）は図1のように構成されている。

【0013】第1発明においては、キー10－1，10－2・・・10－Nの操作に応じたデータをデータ入力手段12が入力し、入力データ表示手段16は入力されたデータを表示器14に表示させる。

【0014】また、アプリケーション記憶手段18には複数のアプリケーションが予め書き込まれ、識別データ記憶手段20はアプリケーション識別用のデータを予め

記憶する。

【００１５】そして、データ照合手段２２は入力されたデータをアプリケーションの識別データと照合し、本人確認手段２４は肯定的な照合結果が得られたときにカード利用者の本人確認を行なう。

【００１６】第２の発明においては、キー１０－１，１０－２・・・１０－Ｎの操作に応じアプリケーション特定データとアプリケーション固有データをデータ入力手段１２が入力し、入力されたアプリケーション特定データと対応したアプリケーション識別用のデータを識別データ読出手段２６が読み出す。

【００１７】データ照合手段２２は入力されたアプリケーション固有データを読み出された各アプリケーションの識別データと照合し、本人確認手段２４は肯定的な照合結果が得られたときにカード利用者の本人確認を行なう。

【００１８】第３に発明においては、肯定的な照合結果が得られたときに該当のアプリケーションについてのみカード利用者の本人確認を本人確認手段２４が行なう。

【００１９】

【作用】第１発明では、キー操作入力のデータをアプリケーションの識別データと照合した結果が肯定的なときに、カード利用者の本人確認が行なわれるので、カード利用者が本人であることと目的の機能（アプリケーション）を確認することが可能となる。

【００２０】第２の発明では、目的の機能がカード利用者により特定されてから、そのアプリケーションに関する識別データとキー操作入力のデータが照合される。

【００２１】第３の発明では、第２発明において肯定的な照合結果が得られた機能についてのみ、カード利用者の本人確認が行なわれる（図３参照）。

【００２２】

【実施例】以下、図面に基づいて本発明にかかるビジュアルＩＣカードの好適な実施例を説明する。

【００２３】図２において、ビジュアルＩＣカード２８には複数のキー１０と表示器１４が設けられており、これらを用いてカード利用者の本人確認がカード単体で行なわれる。

【００２４】このビジュアルＩＣカード２８はその本人確認が行なわれてから図４のカードリーダ・ライタ８４にセットされ、したがって、ＰＩＮデータをキーボード８０から処理装置８２へ入力することを省略してその漏洩を防止できる。

【００２５】本実施例のビジュアルＩＣカード２８には図５のように複数のアプリケーションデータファイル（ＡＤＦ）１，２・・・が格納されており、このカード２８がキャッシュカード及びクレジットカードとして利用される場合には、図６のようにそれらのアプリケーションデータファイル（１，２）が格納される。

【００２６】そして、カード管理情報にはアプリケーションデータファイル１，２・・・の個数が含まれており、これらアプリケーションデータファイル１，２・・・には相異なるＰＩＮデータ（通常は４桁）が各々含まれる（図６では”１２３４”，”５６７８”）。

【００２７】また、ビジュアルＩＣカード２８には図７のキー制御部７０，本人確認部７２，コマンド部７４が設けられており、キー操作で得られたデータはキー制御部１０から本人確認部７２へ入力される。

【００２８】さらに、カード管理情報やアプリケーションデータファイル１，２・・・はコマンド部７４によりアクセスされ、このコマンド部７４で表示部１４が制御される。

【００２９】図８，図９には本人確認部７２で行なわれる処理の内容がフローチャートで示されており、キー入力が確認されると、処理ステータスのフラグがオンされているか否かが判断される（ステップ８００）。

【００３０】このフラグは電源の投入時にオフされており（電源の投入は図２の電源キーを操作することで行なわれる）、そのフラグ状態が確認されたときには、図１０のように５桁長とされたＰＩＮバッファ９０がクリアされる（ステップ８０２）。

【００３１】さらに、アプリケーションデータファイル１，２・・・の数が読み出され（ステップ８０４）、その数が”１”かこれを越えているかが判定される（ステップ８０６）。

【００３２】そして、アプリケーションデータファイルの数が”１”である場合（単機能カードの場合）には、入力データがＰＩＮバッファ９０に格納されてその現行桁がインクリメントされ（ステップ８０８），上記のフラグがオンされる（ステップ８１０）。

【００３３】また、アプリケーションデータファイルの数が”１”を越えている場合（多機能カードの場合）には、キー入力データ（１桁）で示されるファイル名（そのファイルのＰＩＮデータ）が読み出され、セットされる（ステップ８１２）。

【００３４】この後においては、４桁のキーデータがＰＩＮデータとして入力されるまで（ステップ８１４），入力データをＰＩＮバッファ９０に格納してその現行桁をインクリメントする処理（ステップ８１６）が繰り返される。

【００３５】そして４桁のキーデータが（ＰＩＮデータとして）入力されると（ステップ８１４），処理ステータスのフラグがオフされる（ステップ８１８）。

【００３６】次に、セット済みのファイル名（そのファイルに含まれたＰＩＮデータ）とキー操作入力のＰＩＮデータ（先頭４桁．最初に入力された後尾１桁はサフィックスとなる）とが突き合わされ（ステップ８２０．．．アプリケーションデータのファイル数が”１”である場合には、そのファイル名となるＰＩＮデータ），両データの一致が確認されると（ステップ８２

5

2）、確認フラグがオンされ（ステップ８２４）、"Ｒｅａｄｙ"の表示が表示器１４で行なわれる（ステップ８２６）。

【００３７】これに対し、両データの不一致が確認された場合にはその旨が表示器１４で表示され（ステップ８２８，８３０）、両データ不一致の確認が規定の回数だけ繰り返されると、"カード使用不可"の表示が表示器１４で行なわれる（ステップ８３２）。

【００３８】以上のように、最初のキー入力データでアプリケーション数が把握されて対応のデータファイル（１，２・・・のいずれか）が特定され、後続４桁のキー入力データと特定されたデータファイルのＰＩＮデータとが一致したときに、そのアプリケーション（カード機能）についてのみ、本人確認が行なわれる。

【００３９】図６において、"２"に続き"５６７８"のキーデータがＰＩＮデータとして入力されると、アプリケーションデータファイル２のクレジットカード機能について、本人確認が行なわれる。

【００４０】したがって本実施例によれば、ＰＩＮデータの漏洩を確実に防止できる多機能なビジュアルＩＣカード２８を提供することが可能となる。

【００４１】

【発明の効果】以上説明したように本発明によれば、多機能でセキュリティに優れた極めて有用なビジュアルＩＣカードを提供できる。

【図面の簡単な説明】

6

【図１】発明の原理説明図である。

【図２】ビジュアルＩＣカードの外観説明図である。

【図３】発明の作用説明図である。

【図４】実施例のカードを取り扱うシステムの構成説明図である。

【図５】実施例のファイル構造説明図である。

【図６】実施例の具体的なファイル構造説明図である。

【図７】実施例の内部構成説明図である。

【図８】実施例の作用を説明するフローチャート（その１）である。

【図９】実施例の作用を説明するフローチャート（その２）である。

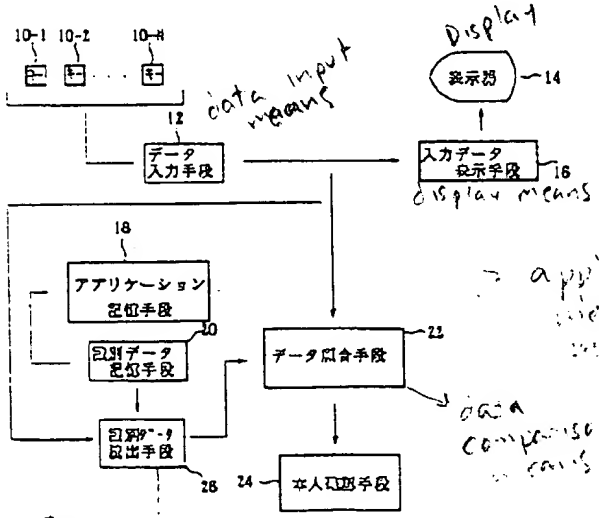
【図１０】実施例で用意されるＰＩＮバッファの構成説明図である。

【図１１】ＩＣカードシステムの構成説明図である。

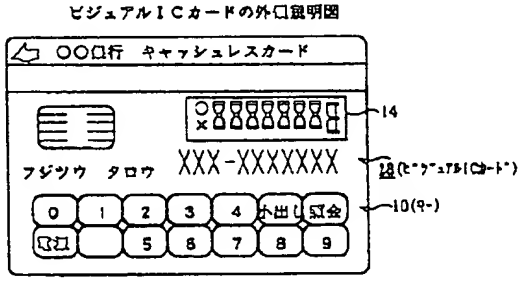
【符号の説明】

１０　キー
１４　表示部
２８　ビジュアルＩＣカード
７０　キー制御部
７２　本人確認部
７４　コマンド部
８０　キーボード
８２　処理装置
８４　カードリーダ・ライタ

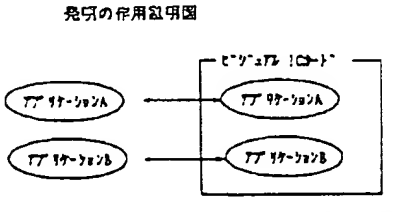
【図１】



【図２】



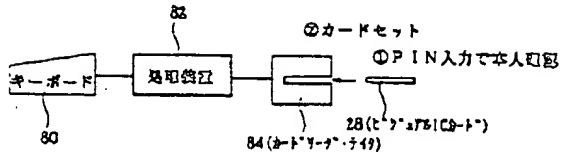
【図３】



<アプリケーション対応で本人確認>

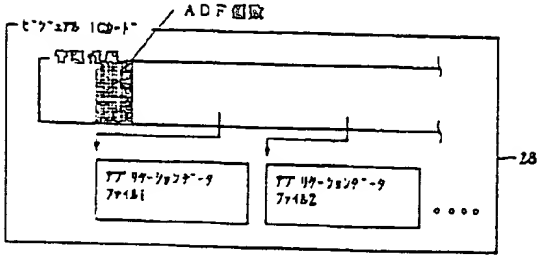
【図4】

実施例のカードを取り扱うシステムの構成説明図



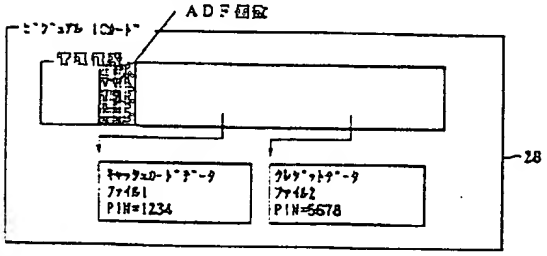
【図5】

実施例のファイル構成説明図



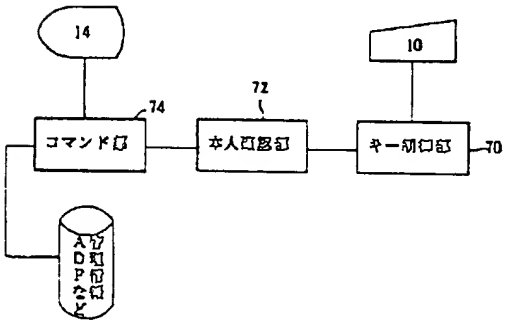
【図6】 file structure

実施例の具体的なファイル構成説明図



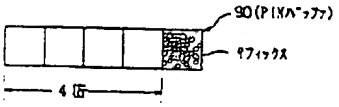
【図7】

実施例の内部構成説明図



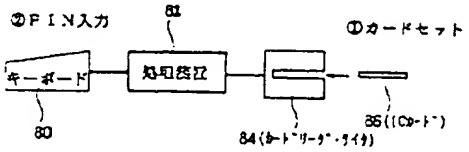
【図10】

実施例で用いられるPINバッファの構成説明図



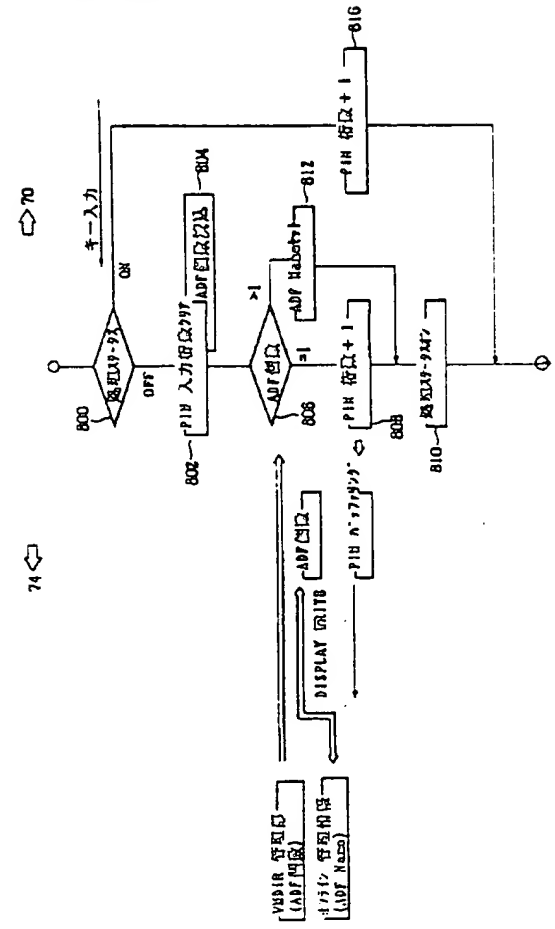
【図11】

ICカードシステムの構成説明図



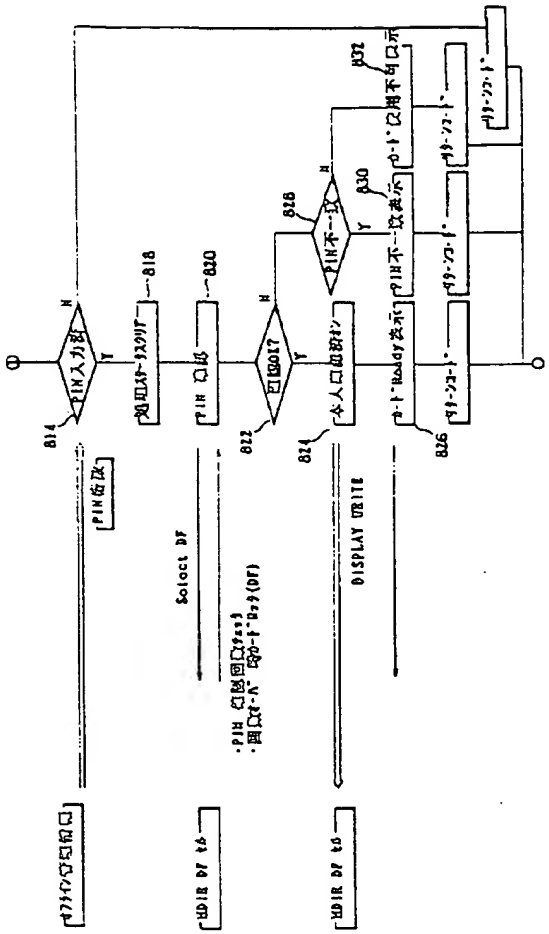
【図8】

実施例の作用を説明するフローチャート



【図9】

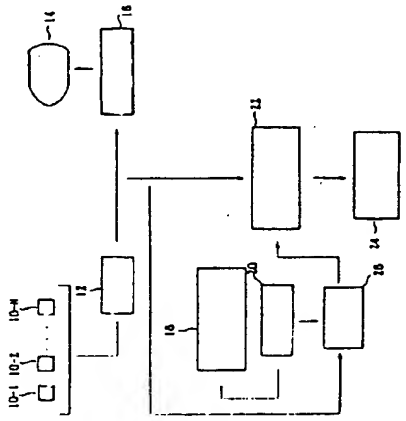
実施例の作用を説明するフローチャート



(54) VISUAL IC CARD
(11) 4-255089 (A) (43) 10.9.1992 (19) JP
(21) Appl. No. 3-36674 (22) 6.2.1991
(71) FUJITSU LTD (72) HIROSHI TANAKA
(51) Int. Cl⁵. G06K19/10,B42D15/10,G06K19/07

PURPOSE: To provide an extremely effective visual IC card having many functions and excellent security with respect to an ID card to be used for a cash card, a credit card, a medical card, etc., especially provided with an input key and a display device.

CONSTITUTION: A data input means 12 inputs data corresponding to the operation of keys 10-1 to 10-N and an input data display means 16 displays the inputted data on a display device 14. Plural applications are previously written in an application storing means 18 and an identification(ID) data storing means 20 previously stores application ID data. A data collating means 22 collates the inputted data with the application ID data and a person-confirming means 24 confirms ~~a~~ card user as ~~its~~ owner when a positive collated result is obtained.

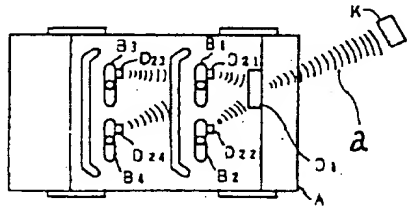


26: ID data reading means

(54) IDENTIFICATION SYSTEM FOR VEHICLE IN/OUT MANAGEMENT
(11) 4-255090 (A) (43) 10.9.1992 (19) JP
(21) Appl. No. 3-9585 (22) 30.1.1991
(71) MEIDENSHA CORP (72) KAZUYUKI KUMAKI
(51) Int. Cl⁵. G07C9/00,B42D15/10,G06F15/21,G06K17/00,G08G1/017

PURPOSE: To automatically execute vehicle identification(ID) and the personal ID of a person getting on a vehicle and to simplify management by making a vehicle ID device loaded on a vehicle to inquire a personal ID card carried by a person getting on the vehicle at the time of passing a gate and transmit a personal ID code together with a vehicle ID code to a vehicle detector.

CONSTITUTION: When a vehicle A passes a gate, the vehicle detector K sends an access signal to a vehicle ID device D_1. The device D_1 transmits an inquiry signal from a transmission part to the inside of the vehicle at the period of about one minute. Persons B_1 to B_4 getting on the vehicle respectively carry respective personal ID cards D_{2i} or the like. After receiving the inquiry signal, respective cards D_{2i} or the like transmit personal ID codes. Each personal ID card is provided with an inherent queue time based on a registered number to prevent the generation of signal collision. The device D_1 transmits the vehicle ID code and the personal ID codes to the detector K. The detector K manages the IN/OUT of the vehicle and the persons getting on the vehicle in accordance with these codes.

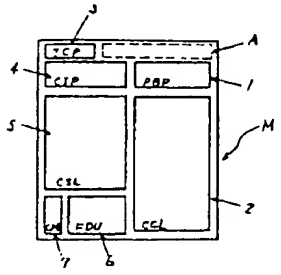


a: signal wave

(54) CASH DISPENSER
(11) 4-255091 (A) (43) 10.9.1992 (19) JP
(21) Appl. No. 3-36901 (22) 6.2.1991
(71) NEC CORP (72) YOSHIMI KITAGAWA
(51) Int. Cl⁵. G07D1/00,G07D9/00

PURPOSE: To improve the operation convenience of a cash dispenser by providing the cash dispenser body with a consumption medium stock rack for storing consumption medium so as to always store the consumption medium.

CONSTITUTION: The cash dispenser body M is provided with a bankbook printer unit 1, a paper money processing unit 2, a card processing unit 4, or the like. The consumption medium stock rack A is arranged on a space position in the upper area of the dispenser body M. The stock rack A is formed by reinforced glass or reinforced plastic so that the inside can be observed and the number of remaining medium can be checked at a glance from the external. The stock rack A is laterally arranged and provided with a bankbook storing rack, a certificate storing rack, a receipt form storing rack, a journal form storing rack, a depositing/paying form storing rack, and a transfer card storing rack. Respective racks are provided with locking keys so as to store important medium.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平4－255089

(43)公開日　平成４年(1992)９月10日

Published

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｋ　19/10				
Ｂ４２Ｄ　15/10	５２１	9111－2C		
Ｇ０６Ｋ　19/07				
		8623－5L	Ｇ０６Ｋ　19/00	R
		8623－5L		J

審査請求　未請求　請求項の数３(全　６　頁)

(21)出願番号　特願平3－36674

(22)出願日　平成３年(1991)２月６日

Application Date Feb. 6, 1991

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中1015番地
(72)発明者　田中　弘
神奈川県川崎市中原区上小田中1015　富士通株式会社内
(74)代理人　弁理士　伊藤　儀一郎

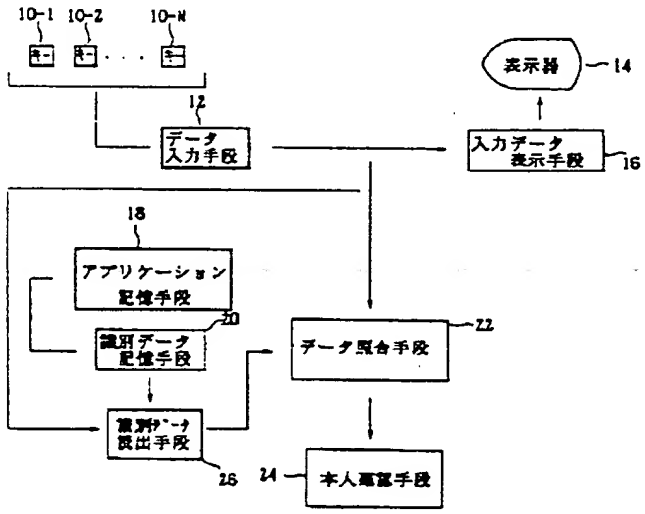
(54)【発明の名称】　ビジュアルＩＣカード

(57)【要約】

【目的】　本発明は、キャッシュカード，クレジットカード，医療カードなどに利用されるＩＣカードにかかり、特に、入力キーと表示器が設けられたＩＣカードに関し、多機能でセキュリティに優れた極めて有用なビジュアルＩＣカードの提供を目的とする。

【構成】　キー１０－１，１０－２・・・１０－Ｎの操作に応じたデータをデータ入力手段１２が入力し、入力データ表示手段１６は入力されたデータを表示器１４に表示させる。アプリケーション記憶手段１８には複数のアプリケーションが予め書き込まれ、識別データ記憶手段２０はアプリケーション識別用のデータを予め記憶する。データ照合手段２２は入力されたデータをアプリケーションの識別データと照合し、本人確認手段２４は肯定的な照合結果が得られたときにカード利用者の本人確認を行なう。

発明の原理説明図



1

【特許請求の範囲】

【請求項１】　キー（１０－１，１０－２・・・１０－Ｎ）の操作に応じたデータを入力するデータ入力手段（１２）と、入力されたデータを表示器（１４）に表示させる入力データ表示手段（１６）と、複数のアプリケーションが予め書き込まれたアプリケーション記憶手段（１８）と、アプリケーション識別用のデータを予め記憶する識別データ記憶手段（２０）と、入力されたデータをアプリケーションの識別データと照合するデータ照合手段（２２）と、肯定的な照合結果が得られたときにカード利用者の本人確認を行なう本人確認手段（２４）と、を有する、ことを特徴としたビジュアルＩＣカード。

【請求項２】　キー（１０－１，１０－２・・・１０－Ｎ）の操作に応じアプリケーション特定データとアプリケーション固有データを入力するデータ入力手段（１２）と、入力されたデータを表示器（１４）に表示させる入力データ表示手段（１６）と、複数のアプリケーションが予め書き込まれたアプリケーション記憶手段（１８）と、アプリケーション識別用のデータを予め記憶する識別データ記憶手段（２０）と、入力されたアプリケーション特定データと対応したアプリケーション識別用のデータを読み出す識別データ読出手段（２６）と、入力されたアプリケーション固有データを読み出されたアプリケーション識別用のデータと照合するデータ照合手段（２２）と、肯定的な照合結果が得られたときにカード利用者の本人確認を行なう本人確認手段（２４）と、を有する、ことを特徴としたビジュアルＩＣカード。

【請求項３】　キー（１０－１，１０－２・・・１０－Ｎ）の操作に応じアプリケーション特定データとアプリケーション固有データを入力するデータ入力手段（１２）と、入力されたデータを表示器（１４）に表示させる入力データ表示手段（１６）と、複数のアプリケーションが予め書き込まれたアプリケーション記憶手段（１８）と、アプリケーション識別用のデータを予め記憶する識別データ記憶手段（２０）と、入力されたアプリケーション特定データと対応したアプリケーション識別用のデータを読み出す識別データ読出手段（２６）と、入力されたアプリケーション固有データを読み出されたアプリケーションの識別データと照合するデータ照合手段（２２）と、肯定的な照合結果が得られたときに該当のアプリケーションについてのみカード利用者の本人確認を行なう本人確認手段（２４）と、を有する、ことを特徴としたビジュアルＩＣカード。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、キャッシュカード，クレジットカード，医療カードなどとして利用されるＩＣカードにかかり、特に、入力キーと表示器が設けられたＩＣカードに関する。

2

【０００２】この種のＩＣカードには入力キーと表示器が設けられており、したがって、それらを用いてカード利用者の本人確認をカード単体で行なうことが可能となる。

【０００３】

【従来の技術】図１１にはＩＣカードシステムが示されており、キーボード８０が処理装置８２（パーソナルコンピュータなど）に設けられている。

【０００４】この処理装置８２にはカードリーダ・ライタ８４が接続されており、ＩＣカード８６はカードリーダ・ライタ８４にセットされる。

【０００５】そして、キーボード８０の操作で処理装置８２にＰＩＮデータが入力されると、この入力データがＩＣカード８６へ送信される。

【０００６】その結果、カード利用者の本人確認が行なわれると、ＩＣカード８６を利用した取引が行なわれる。

【０００７】ところがこのシステムにおいては、本人確認用のＰＩＮデータが処理装置８２へ入力されるので、ＰＩＮデータの漏洩を確実に防止することが困難となる。

【０００８】そこで、図２のように複数のキー１０と表示器１４とを備え、これらキー１０，表示器１４によってカード利用者の本人確認をカード単体で行なえるビジュアルＩＣカード２８が利用される。

【０００９】従来においては、ビジュアルＩＣカード２８に単一のアプリケーションが用意されており、したがって、その用途はキャッシュカード，クレジットカード，医療カードなどのいずれかに限られていた。

【００１０】

【発明が解決しようとする課題】ＭＳカード（磁気カード）にはキャッシュカード，クレジットカードの機能が既に付与されているので、これより能力がはるかに高いビジュアルＩＣカード（２８）にはより豊富な機能が要望される。

【００１１】本発明は上記従来の事情に鑑みてなされたものであり、その目的は、ＰＩＮデータの漏洩を確実に防止できる多機能なビジュアルＩＣカードを提供することにある。

【００１２】

【課題を解決するための手段】上記目的を達成するために、本発明にかかるビジュアルＩＣカード（２８）は図１のように構成されている。

【００１３】第１発明においては、キー１０－１，１０－２・・・１０－Ｎの操作に応じたデータをデータ入力手段１２が入力し、入力データ表示手段１６は入力されたデータを表示器１４に表示させる。

【００１４】また、アプリケーション記憶手段１８には複数のアプリケーションが予め書き込まれ、識別データ記憶手段２０はアプリケーション識別用のデータを予め

3

記憶する。

【００１５】そして、データ照合手段２２は入力されたデータをアプリケーションの識別データと照合し、本人確認手段２４は肯定的な照合結果が得られたときにカード利用者の本人確認を行なう。

【００１６】第２の発明においては、キー１０－１，１０－２・・・１０－Ｎの操作に応じアプリケーション特定データとアプリケーション固有データをデータ入力手段１２が入力し、入力されたアプリケーション特定データと対応したアプリケーション識別用のデータを識別データ読出手段２６が読み出す。

【００１７】データ照合手段２２は入力されたアプリケーション固有データを読み出された各アプリケーションの識別データと照合し、本人確認手段２４は肯定的な照合結果が得られたときにカード利用者の本人確認を行なう。

【００１８】第３に発明においては、肯定的な照合結果が得られたときに該当のアプリケーションについてのみカード利用者の本人確認を本人確認手段２４が行なう。

【００１９】

【作用】第１発明では、キー操作入力のデータをアプリケーションの識別データと照合した結果が肯定的なときに、カード利用者の本人確認が行なわれるので、カード利用者が本人であることと目的の機能（アプリケーション）を確認することが可能となる。

【００２０】第２の発明では、目的の機能がカード利用者により特定されてから、そのアプリケーションに関する識別データとキー操作入力のデータが照合される。

【００２１】第３の発明では、第２発明において肯定的な照合結果が得られた機能についてのみ、カード利用者の本人確認が行なわれる（図３参照）。

【００２２】

【実施例】以下、図面に基づいて本発明にかかるビジュアルＩＣカードの好適な実施例を説明する。

【００２３】図２において、ビジュアルＩＣカード２８には複数のキー１０と表示器１４が設けられており、これらを用いてカード利用者の本人確認がカード単体で行なわれる。

【００２４】このビジュアルＩＣカード２８はその本人確認が行なわれてから図４のカードリーダ・ライタ８４にセットされ、したがって、ＰＩＮデータをキーボード８０から処理装置８２へ入力することを省略してその漏洩を防止できる。

【００２５】本実施例のビジュアルＩＣカード２８には図５のように複数のアプリケーションデータファイル（ＡＤＦ）１，２・・・が格納されており、このカード２８がキャッシュカード及びクレジットカードとして利用される場合には、図６のようにそれらのアプリケーションデータファイル（１，２）が格納される。

【００２６】そして、カード管理情報にはアプリケーションデータファイル１，２・・・の個数が含まれており、これらアプリケーションデータファイル１，２・・・には相異なるＰＩＮデータ（通常は４桁）が各々含まれる（図６では”１２３４”，”５６７８”）。

4

【００２７】また、ビジュアルＩＣカード２８には図７のキー制御部７０，本人確認部７２，コマンド部７４が設けられており、キー操作で得られたデータはキー制御部１０から本人確認部７２へ入力される。

【００２８】さらに、カード管理情報やアプリケーションデータファイル１，２・・・はコマンド部７４によりアクセスされ、このコマンド部７４で表示部１４が制御される。

【００２９】図８，図９には本人確認部７２で行なわれる処理の内容がフローチャートで示されており、キー入力が確認されると、処理ステータスのフラグがオンされているか否かが判断される（ステップ８００）。

【００３０】このフラグは電源の投入時にオフされており（電源の投入は図２の電源キーを操作することで行なわれる）、そのフラグ状態が確認されたときには、図１０のように５桁長とされたＰＩＮバッファ９０がクリアされる（ステップ８０２）。

【００３１】さらに、アプリケーションデータファイル１，２・・・の数が読み出され（ステップ８０４），その数が”１”かこれを越えているかが判定される（ステップ８０６）。

【００３２】そして、アプリケーションデータファイルの数が”１”である場合（単機能カードの場合）には、入力データがＰＩＮバッファ９０に格納されてその現行桁がインクリメントされ（ステップ８０８），上記のフラグがオンされる（ステップ８１０）。

【００３３】また、アプリケーションデータファイルの数が”１”を越えている場合（多機能カードの場合）には、キー入力データ（１桁）で示されるファイル名（そのファイルのＰＩＮデータ）が読み出され、セットされる（ステップ８１２）。

【００３４】この後においては、４桁のキーデータがＰＩＮデータとして入力されるまで（ステップ８１４），入力データをＰＩＮバッファ９０に格納してその現行桁をインクリメントする処理（ステップ８１６）が繰り返される。

【００３５】そして４桁のキーデータが（ＰＩＮデータとして）入力されると（ステップ８１４），処理ステータスのフラグがオフされる（ステップ８１８）。

【００３６】次に、セット済みのファイル名（そのファイルに含まれたＰＩＮデータ）とキー操作入力のＰＩＮデータ（先頭４桁，最初に入力された後尾１桁はサフィックスとなる）とが突き合わされ（ステップ８２０．．．アプリケーションデータのファイル数が”１”である場合には、そのファイル名となるＰＩＮデータ），両データの一致が確認されると（ステップ８２

5

2）、確認フラグがオンされ（ステップ８２４）、”Ｒｅａｄｙ”の表示が表示器１４で行なわれる（ステップ８２６）。

【００３７】これに対し、両データの不一致が確認された場合にはその旨が表示器１４で表示され（ステップ８２８，８３０）、両データ不一致の確認が規定の回数だけ繰り返されると、”カード使用不可”の表示が表示器１４で行なわれる（ステップ８３２）。

【００３８】以上のように、最初のキー入力データでアプリケーション数が把握されて対応のデータファイル（１，２・・・のいずれか）が特定され、後続４桁のキー入力データと特定されたデータファイルのＰＩＮデータとが一致したときに、そのアプリケーション（カード機能）についてのみ、本人確認が行なわれる。

【００３９】図６において、”２”に続き”５６７８”のキーデータがＰＩＮデータとして入力されると、アプリケーションデータファイル２のクレジットカード機能について、本人確認が行なわれる。

【００４０】したがって本実施例によれば、ＰＩＮデータの漏洩を確実に防止できる多機能なビジュアルＩＣカード２８を提供することが可能となる。

【００４１】

【発明の効果】以上説明したように本発明によれば、多機能でセキュリティに優れた極めて有用なビジュアルＩＣカードを提供できる。

【図面の簡単な説明】

6

【図１】発明の原理説明図である。

【図２】ビジュアルＩＣカードの外観説明図である。

【図３】発明の作用説明図である。

【図４】実施例のカードを取り扱うシステムの構成説明図である。

【図５】実施例のファイル構造説明図である。

【図６】実施例の具体的なファイル構造説明図である。

【図７】実施例の内部構成説明図である。

【図８】実施例の作用を説明するフローチャート（その１）である。

【図９】実施例の作用を説明するフローチャート（その２）である。

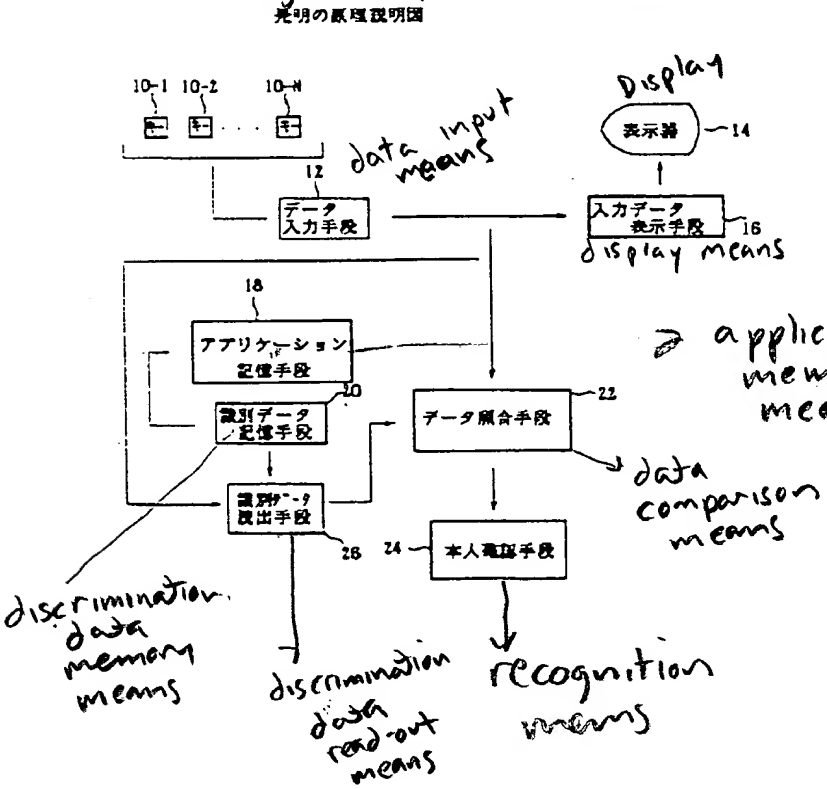
【図１０】実施例で用意されるＰＩＮバッファの構成説明図である。

【図１１】ＩＣカードシステムの構成説明図である。

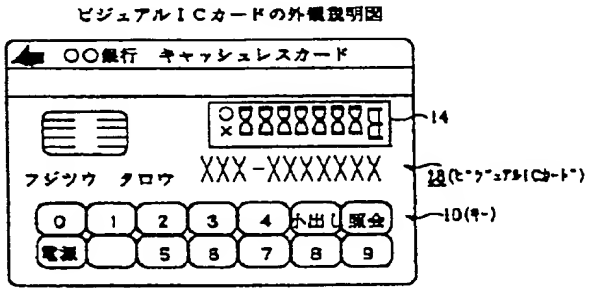
【符号の説明】

１０　キー
１４　表示部
２８　ビジュアルＩＣカード
７０　キー制御部
７２　本人確認部
７４　コマンド部
８０　キーボード
８２　処理装置
８４　カードリーダ・ライタ

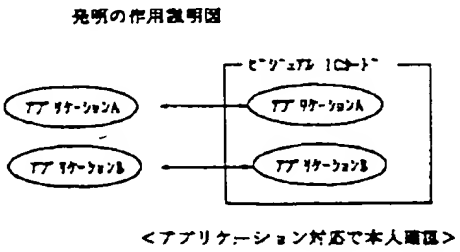
【図１】



【図２】



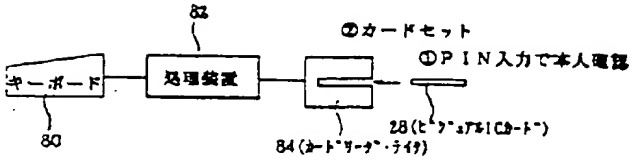
【図３】



<アプリケーション対応で本人確認>

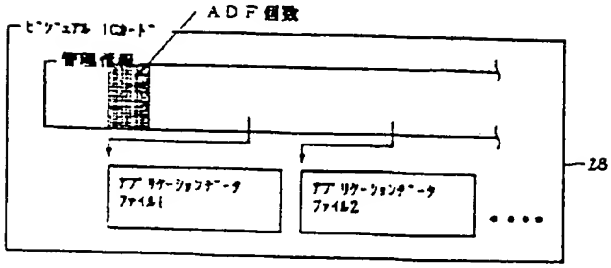
【図４】

実施例のカードを取り扱うシステムの構成説明図



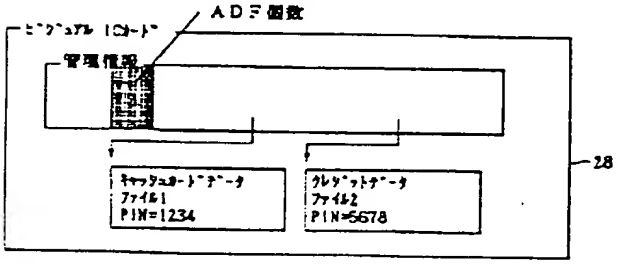
【図５】

実施例のファイル構成説明図



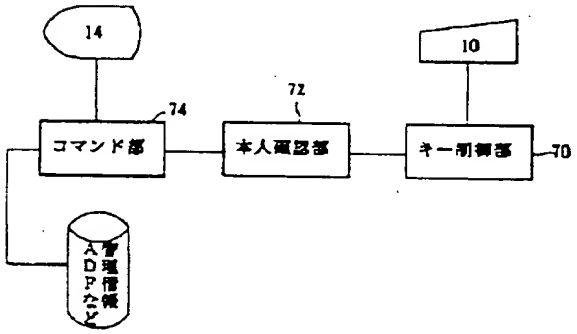
【図６】 file structure

実施例の具体的なファイル構成説明図



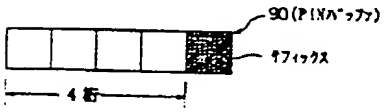
【図７】

実施例の内部構成説明図



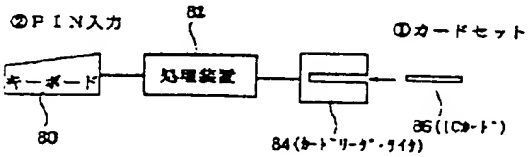
【図１０】

実施例で用意されるＰＩＮバッファの構成説明図



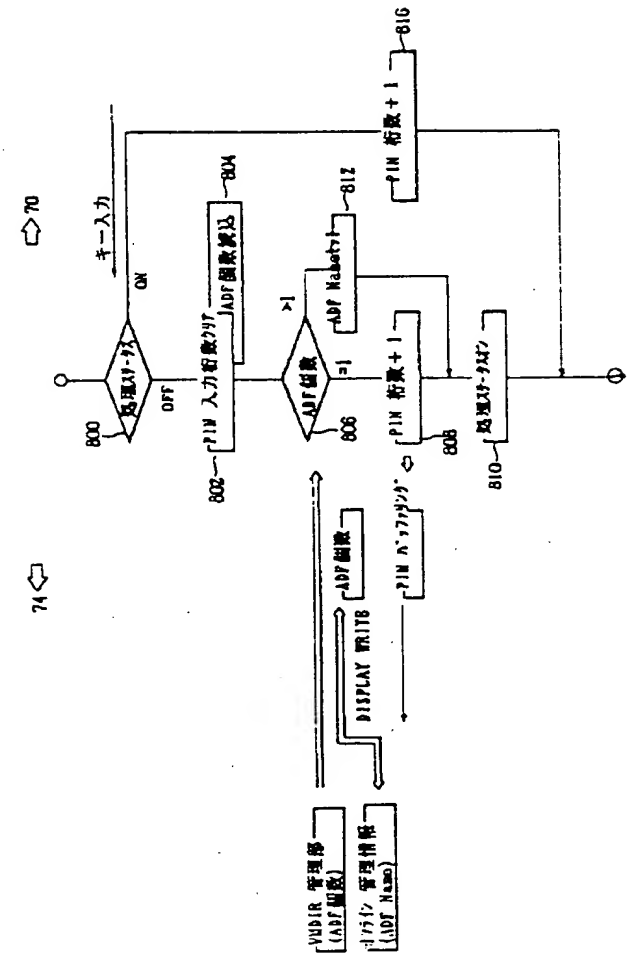
【図１１】

ＩＣカードシステムの構成説明図



【図８】

実施例の作用を説明するフローチャート



【図９】

実施例の作用を説明するフローチャート